BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-119

24 JANUARY 2005

Incorporating Through Change 4, 2 September 2008

Communications and Information

AIR FORCE MESSAGING

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/XCDIG — Certified by: SAF/XCDI (Col Marcus Miller)

Supersedes AFI 33-119, 14 December 2004. — Pages: 38

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-1, Information Resources Management. It sets forth policies regarding the official or authorized use of government-provided electronic messaging systems on both Nonsecure Internet Protocol Router Network (NIPRNet) and SECRET Internet Protocol Router Network (SIPRNet). It identifies the Defense Message System (DMS) as the core-messaging system of record for the Air Force. It provides the roles, standards, and guidance relating to the messaging classes used by the Air Force: organizational DMS High Grade Service (HGS), and Simple Mail Transfer Protocol (SMTP) electronic mail (E-mail) messaging. This instruction applies to all Air Force organizations, personnel, Air National Guard, Air Force Reserve Command, and contractors regardless of the information classification transmitted or received. This instruction provides guidance to differentiate between record and non-record E-mail. Failure to comply with the prohibitions and mandatory provisions of paragraphs **3.9.1.**, **3.9.2.**, and **3.9.3.** by military personnel is a violation of Article 92, Failure to Obey Order or Regulation, Uniform Code of Military Justice (U.C.M.J.). Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Direct technical questions or comments on the contents of this instruction through appropriate command channels to Headquarters Air Force Communications Agency (HQ AFCA/ECSO), 203 W. Losey Street, Room 3100, Scott AFB IL 62225-5222. Refer recommended changes and conflicts between this and other publications to HQ AFCA/EASD, 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, using AF Form 847, Recommendation for Change of Publications. See **Attachment 1** for a glossary of references and supporting information. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, Management of Records; and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at **https://www.my.af.mil/gcss-af61a/afrims/afrims/**. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

SUMMARY OF CHANGES

This change incorporates interim change (IC) Change 4. It provides updated guidance and requirements for using digital signatures when E-mail messages contain embedded hyperlinks and/or attachments. It also provides clearer guidance on encrypting messages. A margin bar indicates newly revised material.

Section A—Roles and Responsibilities

1. Roles and Responsibilities.

1.1. Secretary of the Air Force, Office of Warfighting Integration and Chief Information Officer, Directorate of Warfighter Systems Integration and Deployment (SAF/XCD). SAF/XCD establishes Air Force policy for electronic message administration, policy, and use. Electronic messaging policies include training, planning, maintenance, use, formats, access, security, and record management.

1.2. Headquarters, Air Force Communications Agency (HQ AFCA). HQ AFCA will:

1.2.1. Execute Lead Command responsibilities on Air Force messaging systems as directed by SAF/XCD, to include developing message strategies and concept of operations according to AFI 10-901, *Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR) Lead Command Management*.

1.2.2. Respond to all programmatic Air Force messaging issues.

1.2.3. Provide Headquarters 754th Electronics Systems Group (HQ 754 ELSG), DMS Technical Support Center (DTSC) an approved delete report for Directory Information Tree (DIT) entries that the DTSC has flagged as repeat errors (errors that have been in the DIT over 30 days).

1.2.4. Review the DTSC report of accounts that were not deleted from the approved delete report and forward it to SAF/XCDI.

1.3. HQ 754 ELSG DTSC. HQ 754 ELSG DTSC will:

1.3.1. Run a DIT error scan monthly and provide AFCA the list of entries that were flagged as repeat errors.

1.3.2. Delete erroneous accounts after receiving final approval from AFCA.

1.3.3. Send AFCA the list of accounts that were not deleted from the approved delete report.

1.4. Major Commands (MAJCOM), Direct Reporting Units (DRU), and Field Operating Agencies (FOA). MAJCOMs, DRUs, and FOAs will:

1.4.1. Disseminate and implement Air Force electronic messaging policy within their organizations.

1.4.2. Identify and establish any additional or more restrictive policies for electronic message administration and use within their organizations.

1.5. Wing and Wing-Level Equivalents. Wing and Wing-level equivalents organizations will:

1.5.1. Ensure compliance with Air Force and MAJCOM Electronic Messaging Policy.

1.5.2. As required, identify and establish local policies for electronic message administration and use.

1.5.3. Establish at least one Domain FORTEZZA-based DMS HGS Base Distribution Point (BDP) account to send and receive organizational messages as a “dmsOrganizationalUnit” object under the locality entry in each security domain.

1.5.4. DELETED.

1.6. Commanders. Commanders at all levels will:

1.6.1. Implement Air Force electronic message policy.

1.6.2. Develop local policy and guidance for electronic messaging.

1.6.3. Approve subscription/participation in non-Air Force sponsored e-message news groups in writing based on official duties only.

1.6.3.1. Consider the impact of such services to the network; coordinate through the servicing network communications commander.

1.6.3.2. Approve subscription requests for a period not to exceed one year.

1.6.3.3. Approve each newsgroup individually. Blanket approval for user participation in all news groups is not authorized.

1.6.4. Ensure all message users within their command are educated and trained on the appropriate use of electronic messaging.

1.6.5. Ensure internal storage and control of electronic messages is consistent with Air Force information security and record management policies.

1.6.6. DELETED.

1.6.7. Establish, as a minimum, one DMS HGS E-mail account per base/wing, one account per group commander, one account per squadron commander, one account per two-digit Headquarters Air Force and Secretary of the Air Force (SAF) office, one per two digit MAJCOM and Numbered Air Force Headquarters, and one per FOA and DRU.

1.7. System Administrators. System administrators will:

1.7.1. Comply with Air Force electronic message and network management policies.

1.7.2. Implement Air Force electronic messaging registration procedures according to AFI 33-127, *Electronic Messaging Registration and Authority*.

1.7.3. Make sure the account from which the electronic message was sent is clearly identified in the "FROM" element of the electronic message header. Electronic message senders will not use anonymous accounts or forwarding mechanisms that purposely attempt to conceal the originator of a message unless approved by the commander for the purposes of soliciting anonymous feedback.

1.7.4. Ensure all traffic from and destined for private or limited access military sites (within the .mil domain) is only routed through military controlled networks.

1.8. Electronic Messaging Users. Electronic messaging users will:

1.8.1. Comply with Air Force and MAJCOM electronic messaging policies.

1.8.2. Maintain responsibility for the content of their electronic messages and ensure that messages sent meet Air Force directives regarding acceptable use of electronic messaging.

1.8.3. Maintain sent and received information according to Air Force records management directives: AFMAN 37-123; AFI 33-322, *Records Management Program*; and AFRIMS RDS, (**https://afrims.amc.af.mil/rds_series.cfm**).

1.8.4. Include any special message handling instructions in the message body after the classification (first line) and before the actual text (i.e., "Pass To," "For," "Distribution To," etc.). For DMS

HGS Messages, handling instructions will be included in the "handling instructions" field in the Automatic Digital Network (AUTODIN) tab of the DMS HGS message.

1.8.5. Written approval must be obtained from the commander before subscribing to or participating in electronic message newsgroups except official Air Force internal information products. These products are managed and approved by SAF/PA and accessible from the Air Force Link (**http://www.af.mil**). Using such services without prior approval is misuse of a government system and is subject to disciplinary action. Although this policy recognizes that news groups are a potentially valuable information tool for electronic message users, there is a high potential for abuse. Subscription/participation in e-message news groups will be in support of official duties only.

1.8.6. Report any suspected violations of electronic messaging policy to their supervisor or the information protection office according to Air Force Systems Security Instruction (AFSSI) 5021, *Time Compliance Network Order (TCNO) Management and Vulnerability and Incident Reporting*.

1.8.7. Take appropriate action on non-delivery notices or message rejects to ensure messages reach the intended recipient.

1.8.8. Protect sensitive and classified Air Force information.

1.8.9. Send DMS HGS message NDNs to client support administrators (CSA) for resolution.

1.8.10. Do not auto-forward E-mail from the ".mil" domain to a local Internet service provider.

1.8.11. All contractors assigned to a government office by task order will be provided a government E-mail account and will use the government provided E-mail account to conduct all government business (i.e., queries, responses to other government agencies, etc.) while contracted by the government.

1.9. Client Support Administrators (CSA). CSAs manage the day-to-day operations of the assigned Air Force electronic messaging systems and act as the primary points of contact for electronic messaging troubleshooting. CSAs work with System Administrators and follow DMS-AF and Public Key Infrastructure (PKI) Special Program Office guidance on properly configuring HGS and Medium Grade Service (MGS) clients to minimize adverse bandwidth impacts.

Section B—Air Force Electronic Messaging Classes

2. Air Force Electronic Messaging Classes. Air Force messaging is divided into two classes: Organizational DMS HGS and Simple Mail Transfer Protocol (SMTP) electronic mail (E-mail).

2.1. Organizational DMS (HGS). This class includes organizational (as defined in paragraph **1.6.7.**) messages that require a message release authority, are directive in nature, commit resources (i.e., forces to military action), make formal requests, or provide a command position. Transmit organizational messages via Domain FORTEZZA-based DMS (HGS) messaging accounts.

2.1.1. Sign and encrypt organizational messages to ensure message integrity, non-repudiation, and accountability.

2.1.2. All organizational messages will be prepared in United States (US) Message Text Format (USMTF). Place attachments immediately following the USMTF text.

2.1.2.1. USMTF formats are detailed in Military Standard (Mil Std) 6040, *U.S. Message Text Formatting Program*.

2.1.2.2. A USMTF user may download the Mil Std 6040 from the DISA USMTF web site at **https://disain.disa.mil/usmtf/index.htm**.

2.1.3. Populate the Date-Time-Group, Originator, and Subject fields to identify and reference organizational messages.

2.2. SMTP. This class includes messages by an individual or organizational group/role that do not commit or direct an organization. Official SMTP messages will be digitally signed and encrypted (MGS) (see paragraph **6.**). Unofficial SMTP messages require no digital signature or encryption.

2.3. DELETED.

Section C—Electronic Messaging Policy

3. Electronic Messaging Policy. All government communications systems are subject to monitoring. Members of the Air Force or civilian employees may use a government-provided messaging system for official or authorized use only. Any other use is prohibited.

3.1. AFMAN 37-123 defines official records and electronic records. DOD Regulation 5400.7/AFSUP, *DOD Freedom of Information Act Program*; and AFI 33-332, *Privacy Act Program*, describe when electronic messages are subject to the requirements of the *Freedom of Information Act (FOIA)* and the *Privacy Act of 1974*.

3.2. Adhere to local policy on sending electronic messages to a large number of recipients. Digital images, as well as mass distribution of smaller messages, may delay other traffic, overload the system, and subsequently cause system failure. It is the user's responsibility to manage official record E-mails according to the Air Force Records Disposition Schedule. E-mails may be subject to requests under the FOIA, litigation, and court orders. If requested, individuals are responsible for reviewing messages in E-mail accounts and all backups to locate responsive material. Users are responsible for ensuring the record E-mails are properly filed for access and retrieval.

3.3. Adhere to local policy when sending an electronic message to mail distribution lists. Use web pages or electronic public folders for unofficial electronic messages (i.e., booster club activities, etc.). Only reply to E-mail that absolutely requires a response and minimize the use of the "Reply to All" function.

3.4. Messaging users bear sole responsibility for material accessed and sent.

3.5. Users are responsible for proper coordination and staffing of electronic messaging according to local directives.

3.6. Official taskings will be sent to organizational addresses using HGS. Do not send official taskings to individual addresses.

3.6.1. It is the sender's responsibility to ensure the intended receiver receives the tasking.

3.6.2. It is the receiver's responsibility to ensure the accuracy of the tasking.

3.7. Electronic messaging replaces or supplements formal Air Force formats for communications like official memorandums, messages, orders, taskings, or letters. This includes messages and other com-

munications exchanged between organizational elements in support of command and control, combat support, combat service support, and other functional activities. Users will not add slogans, quotes, special backgrounds, special stationeries, digital images, unusual fonts, etc., to the body of their electronic messages.

3.8. Each office will designate an individual to monitor the organization's mailbox regularly to ensure messages requiring action are promptly acted upon, to include electronic filing and/or destruction, as defined in the organizational file plan and associated table and rule. Each individual should have a unique identifier that the system can authenticate and provide an audit trail. When electronic messaging systems cannot provide a unique identifier, local administrative procedures will provide the audit trail. To assist with providing an audit trail for E-mail users, personnel who send on behalf of the owner of an organizational account will send a copy of all E-mail as "Cc" to the organizational mailbox. This designated individual may be the same individual who monitors the DMS accounts.

3.9. Official Use, Authorized Use, and Use of Subscription Services. Air Force messaging systems support the Air Force mission and are used for official or authorized uses as explained below. For military members, failure to observe the provisions in paragraphs **3.9.1.**, **3.9.2.**, and **3.9.3.** constitutes a violation of Article 92, U.C.M.J. Civilian employees who fail to observe the provisions in paragraphs **3.9.1.**, **3.9.2.**, and **3.9.3.**, are subject to administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions.

3.9.1. Official Use. Official use includes communications, including emergency communications determined necessary in the interest of the Federal government. Official use includes, when approved by the theater commander in the interest of morale and welfare, those personal communications by military members and other Air Force employees who are deployed for extended periods away from home on official business.

3.9.1.1. The following do not constitute official use of government communications systems and are prohibited.

3.9.1.1.1. Distributing copyrighted materials by electronic messaging without consent from the copyright owner. Failure to maintain consent may violate federal copyright infringement laws and could subject the individual to civil liability or criminal prosecution.

3.9.1.1.2. Sending or receiving electronic messages for commercial or personal financial gain.

3.9.1.1.3. Intentionally or unlawfully misrepresenting your identity or affiliation in electronic messaging communications.

3.9.1.1.4. Sending harassing, intimidating, abusive, or offensive material to, or about others.

3.9.1.1.5. Using someone else's identity (user identification [ID] name).

3.9.1.1.6. Causing congestion on the network by such things as the propagation of chain letters, junk E-mails, and broadcasting inappropriate messages to groups or individuals.

3.9.1.1.7. Using government systems for political lobbying.

3.9.1.1.8. Accessing commercial web mail accounts and instant messaging services (i.e., Yahoo, AOL, or MSN mail accounts).

3.9.1.2. Access to personal GI Mail and other instant messaging services on official Air Force web sites (i.e., AF Portal and AF Crossroads) is authorized since these services reside within the ".af.mil" domain and are specifically provided as a risk-mitigated alternative to their commercial counterparts. Wireless devices with web access are authorized to access official Air Force web mail services provided the devices are government issued and accountable.

3.9.2. Authorized Use.

3.9.2.1. In accordance with the DOD 5500.7-R, *Joint Ethics Regulation (JER)*, August 30, 1993, Commanders may authorize, on a limited basis, the use of Air Force E-mail to non-Federal employees as logistical support of an event sponsored by a non-Federal entity, except for fundraising and membership drive events when the Commander determines all of the following:

3.9.2.2. Serves a legitimate public interest.

3.9.2.3. The support does not interfere with the performance of official duties and would not detract from readiness.

3.9.2.4. Conforms to theater combatant commander and MAJCOM policies.

3.9.2.5. Is of reasonable duration and frequency, and whenever possible, is made during personal time.

3.9.2.6. Does not overburden the communications system with large broadcasts or group mailings.

3.9.2.7. Does not reflect adversely on the DOD or the Air Force (such as uses involving pornography, chain letters, unofficial advertising, soliciting or selling, violations of statute or regulation, inappropriately handled classified information or other uses that are incompatible with public service).

3.9.2.8. Does not create a significant additional cost to the DOD or to the Air Force.

3.9.3. Authorized Limited Personal Use Examples. Examples of authorized limited personal use include, but are not limited to:

3.9.3.1. Notifying family members of official transportation or schedule changes.

3.9.3.2. Using government systems to exchange important and time-sensitive information with a spouse or other family members (i.e., scheduling doctor, automobile, or home repair appointments, brief Internet searches, or sending directions to visiting relatives).

3.9.3.3. Educating or enhancing the professional skills of employees, (i.e., use of communication systems, work-related application training, etc.).

3.9.3.4. Sending messages on behalf of a chartered organization, (i.e., unit Booster Club, Base Top 3, Base Company Grade Officers Association, etc.).

3.9.3.5. Limited use by deployed members for morale, health, and welfare purposes.

3.9.3.6. Job searching. Authorized only if related to separations or retirements.

3.9.4. Subscription Services. Internet electronic messaging access grants users the ability to subscribe to a variety of news, mail lists, and discussion groups. These services may include professional groups sponsored by Air Force agencies and other news groups sponsored by non-Air Force

agencies, including the DOD, other Federal agencies, educational institutions, and commercial activities (i.e., product information updates and technical newsletters).

3.9.4.1. Air Force personnel may subscribe to official Air Force-sponsored news, mail lists, and discussion groups. Obtain written approval from the commander before subscribing to or participating in electronic message newsgroups except official Air Force internal information products. These products are managed and approved by SAF/PA and accessible from the Air Force Link (**http://www.af.mil**). Using such services without prior approval is misuse of a government system and is subject to disciplinary action. Subscription or participation in e-message news groups will be in support of official duties only.

3.9.4.2. When an extended absence will not allow access to your electronic messaging account, unsubscribe or suspend mail from any mail lists or news groups. This will alleviate large backlogs of received messages that consume valuable server storage resources.

3.9.4.3. Participation in newsgroups whose content is contrary to the standards set by DOD 5500.7-R (i.e., obscene, offensive, etc.) is prohibited. Unit commanders may direct electronic messaging administrators to set up permanent blocks on a specific site or news group addresses to prevent subscription to such services.

3.10. Message Forwarding (Manual and Automated). If the message was originally encrypted, it should not be forwarded outside the installation's firewall without being encrypted again.

3.10.1. Manual Message Forwarding. To distribute a HGS signed and encrypted message to non-DMS users, the message must be unsigned and decrypted, and converted to SMTP format, before forwarding.

3.10.2. Automated Message Forwarding.

3.10.2.1. Each message will automatically be unsigned/unencrypted and distributed based on profiles loaded in the automated message distribution or profiling system.

3.10.2.2. If required, each message will include manual handling instructions ("Pass To" and "For") at the start of the message text.

3.10.2.3. Do not auto-forward official electronic messages to commercial Internet Service Providers from government computer systems.

3.10.2.4. Automated message forwarding rules or procedures will not be created to send electronic messages to pagers, cell phones, commercial/non-military accounts, Palm Pilots, or other personal digital assistants unless those systems have been approved by the Air Force Certificate To Operate process and are compliant with AFI 33-202, *Network and Computer Security*.

3.10.2.5. After duty hours forwarding of high priority messages will be based on the message transfer system (MTS) priority paradigm of Non-Urgent, Normal, and Urgent. Rules will be set to forward messages with a priority of Urgent to a 24-hour manned location for action.

3.11. Assignment of Precedence. DMS messages will be assigned a precedence from within the Military Message Properties window. The URGENT precedence (Flash, emergency command precedence, or Critic) is reserved for Command Authority use.

3.11.1. DMS HGS message precedence is mapped to a priority within the MTS. The purpose of the mapping is to provide preemption capability within the MTS. The mappings are identified in AFI 33-113, *Managing Air Force Messaging Centers*.

3.11.2. MGS messages will be assigned an importance that is determined by the originator and based upon the desired order of handling of the message by the recipient. MGS importance does not correlate to priority or precedence in the DMS HGS MTS.

3.11.3. The 3 levels of importance are Low, Normal, and High. The default setting is Normal.

3.12. Individual electronic messaging is considered official when the sender is conducting mission related business.

3.13. Special delivery instructions should be included as part of the message text to identify the specific addressee to whom the message is to be delivered. Type "FOR" followed by the name or position title when there is a specific person identified for delivery or "PASS TO" for address instructions to direct the message to a particular organization, unit, or office. For DMS HGS Messages, handling instructions will be included in the "handling instructions" field in the AUTODIN tab of the DMS HGS message.

3.14. Messages with special delivery instructions should not be distributed through normal delivery channels unless specifically requested by the recipient.

3.15. When a member (military, civilian, Guard, Reserve, or Contractor) has another official position (i.e., civilian is a Reservist/Guardsman; contractor is a Reservist/Guardsman or vice versa), the member will be provided two E-mail accounts in order to separate the member's E-mail for each function. For example: John Q. Public, Contr, SAF/XCIFN will have one E-mail identifying him as a contractor and his SMTP address is **john.public.ctr@pentagon.af.mil**. John is also an Air Force Reservist at HAF/A4MM. His reservist E-mail SMTP address will be **john.public@pentagon.af.mil**. Both of his signature blocks will follow the guidance in paragraph **4.**, explicitly.

4. Electronic Message Signature Blocks. Electronic messages, to include official communications such as memorandums (letters), notes, messages, reports, etc., will follow specific formats found in this instruction, Air Force Handbook (AFH) 33-337, *The Tongue and Quill*, AFI 33-321, *Authentication of Air Force Records*, and AFMAN 33-326, *Preparing Official Communications*.

4.1. When using an organizational account subject to access by more than one individual, official electronic messaging will include "//SIGNED//" in upper case before the signature block to signify it contains official Air Force information (e.g., instructions, directions, or policies). This is not to be confused with the digital signature capability in DMS HGS and SMTP MGS messaging. Restrict signature block to name, rank, service affiliation, duty title, and phone numbers (DSN and/or commercial as appropriate) after the "//SIGNED//" entry.

4.2. Senders will include a signature block on all official electronic messaging. For example:

4.2.1. Military Signature Block:

4.2.1.1. Active Duty:

//SIGNED//

RAINY DAYS, Maj, USAF

Branch Chief, Messaging Services

DSN 555-5555 Comm (555)555-5555

4.2.1.2. Military Reservist:

//SIGNED//

Robert Osprey, Lt Col, USAFR

Branch Chief, Employee Services

DSN 555-5555 Comm (555)555-5555

4.2.1.3. National Guard:

//SIGNED//

Joseph A. Chinook, SMSgt, NG

Superintendent, Life Skills

DSN 555-5555 Comm (555)555-5555

4.2.1.4. Active Duty Coast Guard:

//SIGNED//

Harold S. Skywarrior, CWO, CG

OIC, Transportation Flight

DSN 555-5555 Comm (555)555-5555

4.2.2. DoD Civilian Signature Block:

//SIGNED//

Raptor Dominance, GS-12, DAF

Branch Chief, Field Support

DSN 555-5555 Comm (555)555-5555

4.2.3. Contractor Signature Block:

//SIGNED//

Kitty Hawk, Contractor, HQ AFCA/ECFP

DSN 555-5555 Comm (555)555-5555

4.3. DELETED

5. Naming Conventions.

5.1. Simple Mail Transport Protocol (SMTP) Individual. Only *legal names* will be used in the standard format for individual SMTP addresses. This applies to all naming conventions for NIPRNET and SIPRNET. The format for NIPRNET is "FirstName.LastName@base.af.mil" (e.g., john.doe@scott.af.mil); the format for SIPRNET is FirstName.LastName@base.af.smil.mil (e.g., john.doe@scott.af.smil.mil). The Air National Guard (ANG) will have State designations in its Internet domain needed to support inter- and intra-state message traffic flow.

5.1.1. If approved by the local communications squadron, additional information as needed to accommodate other units such as detachments and operating locations may be added to the Internet domain name (e.g., john.doe@det3.scott.af.mil).

5.1.2. Hyphenated names remain hyphenated with a period between the first and last name (e.g., mary.jones-daniel@scott.af.mil).

5.1.3. If duplicate user names exist in the same domain, add a period followed by an integer after the LastName (e.g., john.public.1@scott.af.mil). Use the lowest available integer (i.e. .1, .2, etc.).

5.1.4. DELETED.

5.1.5. Mandatory attributes are required in the Global Address List (GAL) to facilitate the inclusion into the Air Force Directory Services, provide data driven synchronization capability to support the use of PKI and interoperability with other Air Force applications and systems. The mandatory attributes fields for NIPRNET and SIPRNET will be populated only in the format prescribed in this instruction. The mandatory attributes fields are:

5.1.5.1. First Name: Fill in legal first name. Leave blank for objects that are not people. Nicknames or "Known-by" name may not be used. The first letter is capitalized.

5.1.5.2. Middle Initial: Fill in legal middle initial. Leave blank for individuals who don't have a middle name, and for objects that are not people. Only one letter should be used for the initial and it is capitalized. Do not include a period.

5.1.5.3. Last Name: Fill in legal last name. Punctuation is not permitted (except apostrophes and a hyphen as commonly used in married names). Leave blank for objects that are not people. The first letter of each last name is capitalized.

5.1.5.4. Standard Air Force Display Names.

5.1.5.4.1. SMTP Individual. Last Name<COMMA><SPACE>First Name<SPACE>Middle Initial<SPACE>Generation Qualifier<SPACE>Rank/Title<SPACE>Personnel Type <SPACE>Citizenship<SPACE>DoD Component<SPACE>DoD Sub-Component <SPACE>Unit<SLASH>Office Symbol.

5.1.5.4.1.1. Last Name – Legal last name registered with the Defense Manpower Data Center (DMDC). The first letter is capitalized. No nicknames or known-by names may be used.

5.1.5.4.1.2. First Name - Legal first name registered with the DMDC. The first letter is capitalized. No nicknames or known-by names may be used. If no first name, leave blank.

5.1.5.4.1.3. Middle Initial - Legal middle initial registered with the DMDC. Capitalize initial. If no initial, leave blank.

5.1.5.4.1.4. Generation Qualifier – II, III, Jr. Sr., etc. If none, leave blank.

5.1.5.4.1.5. Rank/Title – All ranks listed below in **5.1.5.8.** Contractor leave blank.

5.1.5.4.1.6. Personnel Type – MIL, ANG, RES, CIV, CTR, NAF, AFA, etc. All contractors, Federally Funded Research and Development Center (FFRDC) personnel, or Commercial Vendors will use CTR.

5.1.5.4.1.7. Citizenship – Foreign Nationals Only, US citizens leave blank. When foreign nationals are assigned and authorized access to E-mail, use the 3-letter English country names and codes specified in ISO 3166. GBR, GER, FRA, ITL, etc.

5.1.5.4.1.8. DoD Component – USAF, USA, USN, USMC, USCG, etc.

5.1.5.4.1.9. DoD Sub- Component – ACC, AMC, AETC, AFRC, PACAF, USAFE, etc.

5.1.5.4.1.10. Unit/Office Symbol – Assigned Unit and Office Symbol. 754ELSG/DONE, AF/A1XI, etc.

5.1.5.4.1.11. SMTP Individual Examples:

5.1.5.4.1.11.1. Active Duty Military:
Jones, Robert H MSgt MIL USAF ACC 30IS/DOOE

5.1.5.4.1.11.2. Military Reservist:
Jones, Robert H SMSgt RES USAF AFRC 944CES/CEFO

5.1.5.4.1.11.3. Civilian:
Huck, Keith D Mr. CIV USAF AFCA AFCA/ECSO

5.1.5.4.1.11.4. Contractor:
Smith, John Q. Jr. CTR USAF AFMC 46TW/XPI

5.1.5.4.1.11.5. Foreign National Contractor:
Guttmann, Bert CTR GER USAF USAFE 86MXS/MXMP

5.1.5.4.1.11.6. Air Force Academy (AFA):
Doe, John X C1C MIL USAF USAFA CW/CS30

5.1.5.4.1.11.7. Air National Guard:
Duck, Donald Capt ANG USAF ANG 189 AW/CAT

5.1.5.4.1.11.8. Active Duty/Foreign:
Smith, Eric SSgt MIL GBR USAF AFMC 754ELSG/NONE

5.1.5.4.2. SMTP Organizational. “Organization<SLASH>Office<SPACE>ShortDescriptionOfOffice” (e.g., “ACC/SE Safety”). A space must exist after all numbers in display name (e.g., “1 FW/CC Command Section”). Organizations that are formatted “Det 1 AFRL” must use “AFRL Det 1”. Organizations that have no specific unit designation must be preceded with the base name (e.g., “Gunter Red Cross”).

5.1.5.4.3. SMTP Miscellaneous**.** Any other type of display names not previously addressed above must be preceded with the base name (e.g., "Maxwell Help Desk"). These miscellaneous accounts will be placed in the appropriate Organizational Unit (OU).

5.1.5.5. Phone Numbers. Phone-Business (for Exchange 5.5) or Telephone Number (for Active Directory).

5.1.5.5.1. Phone-Business. Enter the Defense Switched Network (DSN) phone number for the individual or organizational user (e.g., "999-9999"). Do not include the country code. Do not include "DSN". Hyphens are the only special characters or punctuation permitted.

5.1.5.5.2. Phone-Business 2 (for Exchange 5.5) or Telephone Number-Other (for Active Directory). Enter the commercial phone number for the individual or organizational user. Include the area or country code. Either the U.S. or European format may be used (e.g., "(999) 999-9999" or "999.999.9999"). Hyphens, periods, or parenthesis are the only special characters or punctuation permitted. Foreign phone numbers are allowed. ***NOTE***: This field does not show up in the users properties in Active Directory but is used in Exchange 5.5 and Outlook.

5.1.5.6. City. Enter the duty location (e.g., Maxwell, Langley, Pentagon, etc.) or city if no base exists.

5.1.5.7. Company. Enter "USAF" for Air Force government personnel, "USN" for Navy personnel, "USMC" or Marine Corp personnel, "USA" for Army personnel, "USCG" for Coast Guard, Agency name, or "Contractor" for any non-government employee. Contractors may not use the service name they support in this field.

5.1.5.8. Rank. Exchange 5.5 Custom Attributes carry over to the Active Directory. For Organizational accounts, enter the rank as Org, and for Resource accounts, enter the rank as Resource. For individual users, enter appropriate rank as follows:

5.1.5.8.1. Air Force. AB, Amn, A1C, SrA, SSgt, TSgt, MSgt, SMSgt, CMSgt, CMSAF, 2d Lt, 1st Lt, Capt, Maj, Lt Col, Col, Brig Gen, Maj Gen, Lt Gen, Gen.

5.1.5.8.2. Army. PV1, PV2, PFC, CPL, SPC, SGT, SSG, SFC, MSG, 1SG, SGM, CSM, WO1, CW2, CW3, CW4, CW5, 2LT, 1LT, CPT, MAJ, LTC, COL, BG, MG, LTG, GEN.

5.1.5.8.3. Navy. SR, SA, SN, PO3, PO2, PO1,CPO, SCPO, MCPO, CWO-2, CWO-3, CWO-4, ENS, LTJG, LT, LCDR, CDR, CAPT, RADML, RADMU, VADM, ADM.

5.1.5.8.4. Marine. Pvt, PFC, LCpl, Cpl, Sgt, SSgt, GySgt, 1stSgt, MSgt, SgtMaj, MGySgt, CWO2, CWO3, CWO4, CWO5, 2Lt, 1Lt, Capt, Maj, LtCol, Col, BGen, MajGen, LtGen, Gen.

5.1.5.8.5. Government Civilian: Enter the civilian salutation, e.g., Mr., Mrs., Hon., Dr., etc., or leave blank.

5.1.5.8.6. DELETED

5.1.5.8.7. Foreign Nationals. When foreign nationals are assigned and authorized access to E-mail, use the 3-letter English country names and codes specified in ISO 3166. Display name will read Smith, John GBR and formatted as john.smith.GBR@scott.af.mil. Foreign National Contractors will apply both (e.g. john.smith.ctr.GBR@scott.af.mil).

5.1.5.8.8. Special Agents (SA) of the Office of Special Investigations (OSI). SA will be utilized for OSI Special Agents.

5.1.5.9. MAJCOM. (Custom Attribute - Exchange 5.5 Custom Attributes carry over to the Active Directory). Fill in with MAJCOM, DRU, FOA, or Combatant Command name. "HQ" is not to be included. Also, use capital letters where appropriate for MAJCOMs, DRUs, etc.

5.1.6. Entries in the Air Force GAL will be restricted to government domains only, (i.e., .mil, .gov, .us).

5.2. Simple Mail Transfer Protocol (SMTP) Organizational. An organizational account will use a combination of the standard organizational abbreviation and standard Air Force office symbol to form the UserID. Obtain the standard organizational abbreviation from the *Air Force Address Directory* at **https://private.afca.af.mil/afdir/**. Standard Air Force office symbols are also obtained from the Air Force Address Directory at **https://private.afca.af.mil/afdir/fas.cfm**.

5.2.1. The standard naming convention format for organization SMTP message addressing is organization.officesymbol@base.af.mil (e.g., af.ilc@pentagon.af.mil). The ANG will have State designations in its Internet domain needed to support inter- and intra-state message traffic flow.

5.2.2. If approved by the local communications squadron, additional information as needed to accommodate other units such as detachments and operating locations may be added to the Internet domain name (e.g., afca.gcom@afca.scott.af.mil).

5.2.3. UserIDs for units at wing, group, and squadron level will consist of the standard organizational abbreviation and standard Air Force office symbols separated by a period (e.g., the Commander, 10th Wing, is represented as 10WG.CC and the Commander, 10th Communications Group, is represented as 10CG.CC. You may add additional information as needed to accommodate other units such as detachments and operating locations (e.g., the Commander, Detachment 1, 10th Wing, is represented as 10WG.DET1.CC.

5.2.4. UserIDs for higher headquarters will consist of the headquarters standard organizational abbreviation and standard Air Force office symbol separated by a period (e.g., USAF.ILC).

5.3. Organizational Unit (OU) and Common Name (CN). Bases should create top-level OUs for each organization on base directly subordinate to the locality name. Subordinate-level OUs should be created for the offices down to whatever level there is a requirement. Refer to **Attachment 2** for additional descriptions and details on Air Force OU and CN conventions.

6. Digitally Signing and Encrypting SMTP (MGS) E-Mail.

6.1. Digitally signing and encrypting SMTP E-mail using DoD PKI certificates are two measures used to secure the network. A signed and encrypted E-mail takes advantage of DoD's robust and trusted PKI, and as signing and encrypting becomes a routine procedure, the threat of malicious E-mail is reduced.

6.1.1. Digitally Signing E-mails. Digital signatures shall be used whenever it is necessary for the recipient to be assured of the sender's identity, have confidence the message has not been modified, or when nonrepudiation is required. Messages containing only unofficial information and not containing an embedded hyperlink and/or attachment should not be digitally signed. Refer to guidance established in AFI 33-321 for policies concerning the authenticating of E-mails. Examples of messages that should be digitally signed include:

6.1.1.1. Formal direction to a government employee or contractor.

6.1.1.2. Messages that stipulate an Air Force official position on any matter.

6.1.1.3. Messages that commit to, authorize, or deny the use of funds in some manner.

6.1.1.4. E-mails from user accounts and systems which contain an embedded hyperlink and/or attachment. Plain-text references to URL's do not require digital signature but they are recommended.

6.1.2. Encrypting E-mail. DoD PKI-based encryption is not authorized for protecting classified information on systems not approved for that use. Encryption increases bandwidth and resource requirements; therefore, e-mail encryption should be used to protect the following types of information, and the number of E-mail recipients should be kept to a minimum:

6.1.2.1. For Official Use Only (FOUO).

6.1.2.2. Privacy Act Information.

6.1.2.3. Personally Identifiable Information (PII).

6.1.2.4. Individually identifiable health, DoD payroll, finance, logistics, personnel management, proprietary, and foreign government information.

6.1.2.5. Contract data.

6.1.2.6. Export controlled technical data or information.

6.1.2.7. Operations Security (OPSEC) information. Encrypt critical information, OPSEC indicators, and other sources of information. For additional guidance on OPSEC requirements see AFI 10-701, Operations Security.

6.1.2.8. Information specified for encryption by domain owners pertaining to your individual areas of responsibility, see AFPD 33-4, Enterprise Architecting.

6.2. Wireless Handheld Devices. When deciding whether to send signed or encrypted E-mails to recipients using authorized wireless handheld devices, users must be aware that intended recipients will not be able to read or forward that E-mail from handheld devices such as Blackberry, Microsoft Mobile Device, etc., unless they are properly configured for DoD PKI compatibility. Handheld devices used to originate E-mail containing information meeting the criteria in paragraphs **6.1.1.** and **6.1.2.** shall be configured for encrypting and signing E-mails using DoD PKI certificates.

7. Message Management and Destruction.

7.1. Message Management. Electronic messages must be managed, stored, and deleted from the E-mail system after copying to a record keeping system according to AFMAN 37-123. If a digitally signed and/or encrypted official record is to be preserved, the user must follow procedures established by the Air Force Records Officer, pursuant to AFI 33-322, regarding the retention of information necessary to validate the digital signature, and to ensure that the record is accessible and available.

7.1.1. Preserve the content, context, and structure of records in a useable format for their authorized retention period. A complete electronic messaging record will include the message itself, attachments (e.g., word processing and other electronic documents transmitted with the message), and transmission data (e.g., originator, recipients, addresses, date, and time).

7.1.2. Make records easily accessible by individuals who have an official need to access them.

7.1.3. Preserve electronic messaging data that identifies users by codes, nicknames, addresses, and distribution lists to enable identification of the originator and recipients of record messages.

7.1.4. Maintain receipts that show delivery and disposition status (e.g., delivered, opened, replied, deleted, etc.) of all official messages kept according to AFMAN 37-123.

7.1.5. Maintain receipts and acknowledgments with the original message.

7.1.6. Arrange electronic message records according to the approved file plan.

7.1.7. Ensure federal records sent or received on electronic messaging systems outside organizational control are preserved. Ensure reasonable steps are taken to capture available transmission and receipt data needed by the agency for record-keeping purposes.

7.1.8. Use backup tapes of messages for security, system restoration and short-term archiving of official record E-mail not to exceed 120 days. Users are required to retain official record emails by filing in an approved electronic record keeping system. If an approved electronic record keeping system is not available, users will print the official record E-mails to paper copy and file.

7.2. Message Destruction.

7.2.1. Protect messages from unauthorized or unintentional disclosure or destruction.

7.2.2. Users must destroy messages according to AFRIMS RDS instructions located at **https://afrims.amc.af.mil/rds_series.cfm**. Message destruction at the system administration level will occur every 90 days.

7.3. Management of both official and individual messages is determined by the Chief of an Office of Record and is based upon the message originator's authentication authority.

7.3.1. In determining whether a message is a record or not, focus on the content of the information and not on the method used to send it. If the information (content) in the message would have been filed if it had been created on paper, then the message should also be filed or archived. (Prior to electronically filing or archiving, encrypted messages will be decrypted.) In some cases an individual message may become background information to the final decision or recommendation. In other cases the message may be managed in a suspense document until all comments are received and incorporated into a final document, then filed under the appropriate table and rule in Air Force Records Disposition Schedule.

7.3.2. Electronically save official messages in an approved electronic record keeping system or print and place them in the official files when they: contain unique, valuable information; convey statements of policy; provide rationale for official decisions or actions; provide evidence of functions of the government; or document a business transaction.

8. Security.

8.1. The information below describes programs and measures to help protect information from unauthorized disclosure.

8.1.1. Do not setup E-mail auto-forwarding to non-DOD mail accounts.

8.1.2. Address all security issues and incidents to the Computer Systems Security Officer.

8.1.3. When required, sanitize, destroy, and release storage media according to AFSSI 5020, *Remanence Security*.

8.2. Policy.

8.2.1. Safeguard sensitive and classified information at all times. Apply safeguards so information is accessed only by authorized persons, is used only for its intended purpose, retains its content integrity, and is marked properly as required by Office of Management and Budget (OMB)/ Information Security Oversight Office (ISOO) Directive No. 1, *Classified National Security Information;* DOD 5200.1-R, *Information Security Program*, January 1997; and AFI 31-401, *Information Security Program Management*.

8.2.2. Safeguard all information to prevent tampering, loss, destruction, fraud, waste, and abuse.

8.2.3. Safeguard information and electronic messaging system resources against sabotage, denial of service, espionage, misappropriation, misuse, or release to unauthorized persons. Continually employ administrative, procedural, physical, environmental, personnel, communications, emanations, operations, information, and computer security safeguards.

8.2.4. Ensure the mix of safeguards selected for electronic messaging systems that process sensitive or classified information meets the minimum requirements as set forth in DOD Directive (DODD) 8500.1, *Information Assurance (IA)*, October 24, 2002.

8.2.5. Access by foreign nationals to US Government-owned or US Government-managed information systems depends on the Foreign National's category as defined in AFI 33-202.

8.2.6. If employed by the foreign government, allied or coalition forces, then the Office of the Secretary of Defense will approve network access.

8.3. Operations Security (OPSEC). Encrypt critical information, OPSEC indicators, and other sources of information before transmission. For additional guidance on OPSEC requirements see AFI 10-1101, *Operations Security*.

8.4. Privacy Act Information. The Privacy Act of 1974 requires agencies to provide safeguards to ensure the security and confidentiality of records and to protect individuals against an invasion of personal privacy. As such, the electronic collection, maintenance, use, and dissemination of personal information directly affect the privacy of an individual. Refer to AFI 33-332 and AFI 33-129, *Transmission of Information Via the Internet*, for the appropriate procedures required to send Privacy Act information across the Internet.

8.4.1. Exercise caution before transmitting personal information over E-mail to ensure the message is adequately safeguarded. Some information may be so sensitive and personal that E-mail may not be the proper way to transmit it. When sending personal information over E-mail within DOD, ensure:

8.4.1.1. There is an official need.

8.4.1.2. All addressees (including "cc" addressees) are authorized to receive it under the Privacy Act.

8.4.1.3. It is protected from unauthorized disclosure, loss, or alteration.

8.4.2. E-mails shall be encrypted when they contain FOUO and Privacy Act Information. Additional protection methods may include password protecting the information in a separate

Microsoft Word™ document. When transmitting personal information over E-mail, add For Official Use Only ("FOUO") to the beginning of the subject line, followed by the subject, and apply the following statement at the beginning of the E-mail: "This E-mail contains For Official Use Only (FOUO) information which must be protected under *The Privacy Act* and AFI 33-332." Do not indiscriminately apply this statement to E-mails. Use it only in situations when you are actually transmitting personal information. DoD Regulation 5400.7/ AFSUP provides additional guidance regarding FOUO information. Personal information may not be disclosed to anyone outside DoD unless specifically authorized by *The Privacy Act*.

8.4.3. Do not send Privacy Act information to distribution lists or group E-mail addresses unless each member has an official need to know the personal information. Official SMTP messages will be digitally signed and encrypted (MGS) (see paragraph **6.**). Before forwarding E-mails you have received that contain personal information, verify that your intended recipients are authorized to receive the information under *The Privacy Act*.

8.4.4. *Freedom of Information Act (FOIA)*. Do not send information normally exempt under FOIA across the Internet without an appropriate level of protection to prevent unintentional or unauthorized disclosure. Refer to DOD 5400.7-R/AFSUP for additional guidance or consult your local FOIA representative. Refer to AFI 33-129 for the appropriate level of protection.

8.4.5. Protecting Electronic Message Addresses. Do not indiscriminately release electronic messaging addresses. Lists of individual electronic messaging addresses are exempt from disclosure under the FOIA as information, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy (FOIA Exemption 6) (Reference DOD Regulation 5400.7/AFSUP). Reference AFI 33-129 for guidance on the inclusion of electronic messaging addresses in web pages.

8.5. Physical Security. The electronic messaging system administrator must set up procedures defining the control, security, access, and maintenance of all electronic messaging storage media.

8.6. Marking Classified Electronic Messaging. Mark all classified electronic messages according to DOD 5200.1-R and DOD 5200.1-PH, *DOD Guide to Marking Classified Documents*, April 1997.

8.6.1. Mark all classified electronic messages with an overall classification in the subject line. The overall classification must reflect the highest classification of the information contained within the entire transmission--to include all attachments.

8.6.2. Mark all attachments, paragraphs, and subparagraphs with their classification in the same manner as normal correspondence. **Attachment 3** contains detailed procedures for marking classified electronic messages and attachments.

8.7. Message Declassification. Classified messages must contain declassification or downgrading instructions at the end of the message text. See AFI 31-401 for additional guidance.

8.8. Classified Electronic Message Destruction.

8.8.1. Destroy classified messages when no longer required. If the classified message is an official record, destroy it only after the retention period in Air Force Records Disposition Schedule has expired.

8.8.2. Top Secret Control Officers use AF IMT 143, **TOP SECRET Register Page**, or another approved form (e.g., AF IMT 310, **Document Receipt and Destruction Certificate**) to record the destruction of TOP SECRET electronic messages.

8.8.3. When you must keep a record of destroyed SECRET and CONFIDENTIAL materials, use either AF IMT 310 or AF IMT 1565, **Entry, Receipt and Destruction Certificate**.

8.8.4. Destroy residual classified information by purging or by destroying electronic media according to AFSSI 5020.

8.9. Special Handling Requirements. Do not transmit unclassified information that requires special handling on or to systems not approved for that purpose.

8.9.1. General or flag officers and civilians of equivalent rank may originate PERSONAL FOR electronic messages from organizational HGS accounts and SMTP MGS accounts. SMTP MGS accounts are encouraged over organizational HGS accounts. Use the format "PERSONAL FOR (recipient's name) FROM (originator's name)" in the message subject line. Reference Allied Communications Publication (ACP) 121, (C) *DCS Operating Procedures* (U).

8.9.2. Transmission of unclassified information on classified networks is authorized unless specifically prohibited by the network operating instructions. The guidelines listed in **Attachment 4** apply to all unclassified electronic messages sent across a classified network.

8.9.3. Identify all Privacy Act and FOUO electronic messages in the subject line with FOUO.

9. Information Collections, Records, and Forms or Information Management Tool (IMT) .

9.1. Information Collections. Information Collections. Information collections created by this publication are exempt from licensing according to AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections*.

9.2. Records.

9.2.1. Records pertaining to AF Form 143, *TOP SECRET Register Page*, or another approved form (e.g., AF Form 310, *Document Receipt and Destruction Certificate*) to record the destruction of TOP SECRET electronic messages (paragraph **8.8.2.**) are created by this publication. Retain and dispose of these records according to AFRIMS RDS, Table 31-04, Rule 16, located at **https://afrims.amc.af.mil/rds_series.cfm**.

9.2.2. Records pertaining to AF Form 310 or AF Form 1565 to record destroyed SECRET and CONFIDENTIAL materials (paragraph **8.8.3.**) are created by this publication. Retain and dispose of these records according to AFRIMS RDS, Table 31-04, Rule 20, located at **https://afrims.amc.af.mil/rds_series.cfm**.

9.3. Forms or IMTs (Adopted and Prescribed).

9.3.1. Adopted Forms or IMTs. AF Form 847, **Recommendation for Change of Publications**, AF IMT 143, **TOP SECRET Register Page**, AF IMT 310, **Document Receipt and Destruction Certificate**, and AF IMT 1565, **Entry, Receipt and Destruction Certificate,** are adopted in this publication.

9.3.2. Prescribed Forms or IMTs. No forms or IMTs are prescribed by this publication.

MICHAEL W. PETERSON, Lt Gen, USAF
Chief of Warfighting Integration
and Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

OMB/ISOO Directive No. 1, *Classified National Security Information*

Privacy Act of 1974

Freedom of Information Act

Title 44, U.S.C. § 3301, *Definition of Records*

ACP 121, (G) *Communications Instructions-General* (U), October 2004

DoD 5200.1-PH-1, *Classified Information Nondisclosure Agreement (SF 312)*, May 26, 2000

DoD 5200.1-R, *Information Security Program*, January 14, 1997

DoD 5500.7-R, *Joint Ethics Regulation (JER)*, August 30, 1993, w/Ch 1, November 2, 1994; Ch 2, March 25, 1996; Ch 3, December 12, 1997; Ch 4, August 6, 1998, Ch 5, October 25, 2005; Ch 6, March 23, 2006

DoDD 8500.1, *Information Assurance (IA)*, October 24, 2002

DoD 5400.7-R/AF Supplement, *DOD Freedom of Information Act Program*, 24 June 2002

Mil Std 6040, *U.S. Message Text Formatting (USMTF) Program*, November 3, 2006

AFPD 31-4, *Information Security*, 1 September 1998

AFPD 33-1, *Information Resources Management*, 27 June 2006

AFPD 33-3, *Information Management*, 28 March 2006

AFI 10-901, *Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR) Lead Command Management*, 22 March 2001

AFI 10-701, *Operations Security (OPSEC)*, 30 September 2005

AFI 31-401, *Information Security Program Management*, 1 November 2005

AFI 33-113, *Managing Air Force Messaging Centers*, 6 February 2007

AFI 33-127, *Electronic Messaging Registration and Authority*, 1 May 1998

AFI 33-129, *Web Management and Internet Use*, 3 February 2005

AFI 33-138, *Enterprise Network Operations Notification and Tracking*, 28 November 2005

AFI 33-202, Volume 1, *Network and Computer Security*, 3 February 2006 (Through Change 4, 10 January 2007)

AFI 33-321, *Authentication of Air Force Records*, 27 July 2006

AFI 33-322, *Records Management Program*, 7 October 2003

AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections*, 1 June 2000

AFI 33-332, *Privacy Act Program*, 29 June 2004

AFMAN 33-326, *Preparing Official Communications*, 1 November 1999

AFMAN 37-123, *Management of Records*, 31 August 1994 (will become AFMAN 33-363)

AFH 33-337, *The Tongue and Quill*, 1 August 2004

AFRIMS RDS, **https://webrims.amc.af.mil/rds_series.cfm**

AFSSI 5020, *Remanence Security*, 20 August 1996

AFSSI 5021, *Time Compliance Network Order (TCNO) Management and Vulnerability and Incident Reporting*

Abbreviations and Acronyms

ACP—Allied Communications Publication

AD—Active Duty

AFCA—Air Force Communications Agency

AFH—Air Force Handbook

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFRIMS—Air Force Records Information Management System

AFSSI—Air Force Systems Security Instruction

ANG—Air National Guard

APO—Army/Air Force Post Office

AUTODIN—Automatic Digital Network

BDP—Base Distribution Point

CN—Common Name

CSA—Client Support Administrator

DISAC—Defense Information Systems Agency Circular

DIT—Directory Information Tree

DMS—Defense Message System

DN—Distinguished Name

DoD—Department of Defense

DoDD—Department of Defense Directive

DRU—Direct Reporting Unit

DSN—Defense Switched Network

DTSC—DNS Technical Support Center

E-mail—Electronic Mail

FFRDS—Federally Funded Research and Development Center

FOA—Field Operating Agency

FOIA—Freedom of Information Act

FOUO—For Official Use Only

GAL—Global Address List

GEOREF—Geographic Reference

HAF—Headquarters Air Force

HGS—High Grade Service

HQ 754 ESG—Headquarters 754th

IA—Information Assurance

ID—Identification

IOC—Officer-in-Charge

ISOO—Information Security Oversight Office

JER—Joint Ethics Regulation

MAJCOM—Major Command

MGS—Medium Grade Service

MTS—Message Transfer System

NCOIC—Noncommissioned Officer-In-Charge

NIPRNET—Nonsecure Internet Protocol Router Network

NMI—No Middle Initial

NT—New Technology

O/R—Originator/Recipient

OCONUS—Outside the Continental United States

OIC—Officer-In-Charge

OMB—Office of Management and Budget

OPSEC—Operations Security

OSI—Office of Special Investigations

OU—Organizational Unit

PII—Personally Identifiable Information

PKI—Public Key Infrastructure

PLA—Plain Language Address

RDS—Records Disposition Schedule

SA—Special Agents

SAF—Secretary of the Air Force

SIPRNET—SECRET Internet Protocol Router Network

SMIME—Secure Multipurpose Internet Mail Extension

SMTP—Simple Mail Transfer Protocol

SRA—Sub-Registration Authority

SU—Sensitive Unclassified

TCNO—Time Compliance Network Order

TSS—Traffic Service Station

U.C.M.J.—Uniform Code of Military Justice

US—United States

U.S.C.—United States Code

USMTF—United States Message Text Format

WM—Workgroup Manager

Terms

Base Distribution Point (BDP)—An account created under the base locale for each site to receive signed and encrypted messages. The BDP is used as a default address when an organization's account or its parent unit account is not available. Use it to receive en masse distribution messages that are not specifically addressed to any organization (e.g., All Military Activities [ALMILACT]). Bases will make distribution of such messages to the recipients.

E-mail Messages are Records—when they are both (1) created or received by an employee of the agency in the transaction of agency business, and (2) required by the Air Force Records Disposition Schedule to be preserved, or are appropriate for preservation, as evidence of the agency's organization and activities, or because of the value of the information they contain.

Individual Messaging Account—An electronic messaging account created for and accessed by a single individual only.

Naming Convention—A method of uniquely identifying an electronic messaging address on a network.

Newsgroup—Internet resources by which individuals interested in a particular topic may read and post messages that are accessed, read, and responded to by other Internet users. Newsgroups are either moderated (messages are screened for appropriateness before posting), or unmoderated (all messages are posted, regardless of content).

Nonrecord Materials—Government-owned documentary materials that do not meet the conditions of record status (see Subsection 1222.34(b)) or that are specifically excluded from status as records by statute (see Title 44 United States Code [U.S.C.] 3301, *Definition of Records*).

Official records—Defined in Title 44 U.S.C. § 3301 as: "All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the U.S. Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government, or because of the informational value of data in them."

Organizational Messaging Account—An electronic messaging account used to receive and send organizational messages. Send official correspondence that tasks an organization to its organizational account.

Personal Papers—Documentary materials, or any reasonably separate portion thereof, of a private or nonpublic character that do not relate to, or have an effect upon, the conduct of agency business. Personal papers are excluded from the definition of Federal records and are not owned by the Government. Personal papers shall be clearly designated as such and shall at all times be maintained separately from the office's records. If information about private matters and agency business appear in the same document, the document shall be copied at the time of receipt, with the personal information deleted, and treated as a Federal record (see Subsection 1222.36(b) (c) (d)).

Sensitive Information—Information requiring special protection from disclosure that could cause embarrassment, compromise, or threat to the security of the sponsoring power.

Traffic Service Station (TSS) Account—A TSS account is created under the organization locale to provide each organization with a DMS capability. The TSS account is configured to receive signed and encrypted messages. The TSS account allows organizational messages to be delivered to an organization for further distribution (automated or manual). Messages sent to an organization's TSS mailbox must include distribution instructions in the body of the message.

Attachment 2

ORGANIZATIONAL UNIT (OU) AND COMMON NAME (CN) NAMING CONVENTION

A2.1. Organizational and Site Naming Conventions.

A2.1.1. Organization Naming Convention. Set the DMS-AF and non-DMS-AF site Organization Name to read "ORGANIZATION" (spelled out in all uppercase letters) during the initial installation.

A2.1.2. Site Naming Convention. All organizations will use site names that are unique within their organization. Spell out the main DMS-AF site name in upper case (e.g., LANGLEY). This is the same convention recommended for the base New Technology (NT) Domain and the Domain Name Server. If this convention was already used as a non-DMS-AF site name, then the DMS-AF site should choose an alternate site name of "SITE-NAME AFB" (e.g., LANGLEY AFB).

A2.1.3. Primary Server Naming Convention. The DMS-AF primary server and its backup will conform to the 8-character naming convention (**Table A2.1.**).

Table A2.1. Primary Server Naming Convention.

Character	Description
1	One-character service/agency code representing the maintenance provider (e.g., K for DISA-purchased servers, F for Air Force-purchased servers).
2	Represents the type of DMS component (e.g., servers are always S).
3-6	Four-character code (upper case) conforming to DISAC 310-65-1 geographic reference (GEOREF) code. This authoritative source identifies the physical location of the server.
7-8	Two-character code used to identify a specific server at a location. The code 01 is reserved for use as the DMS sensitive unclassified (SU) primary server and 02 is reserved for use as the DMS SU backup server. The SECRET community will use 76 and 77 as the primary and backup server identification codes, respectively. Use a base 34 number (X_{34}) if you need to identify more than 99 servers. Obtain the X_{34} number by using a combination of 10 numbers (i.e., 0 - 9) and 24 letters (i.e., A - K, M, N, and P - Z; the letters L and O are reserved--do not use them). **Example:** A non-DMS-AF server on Gunter AFB would be named "FSJUBJ04" where F = Air Force-purchased and maintained, S = server, JUBJ = Gunter AFB GEOREF code, and 04 = the sequential identification number of the server.

A2.1.4. Public Folder Naming Convention. Only the base name in the following format should be used at the top level (e.g., Langley AFB). Failure to adhere to this convention will cause replication and possibly conflicting folder names. Below the base name, there is no set format.

A2.2. X.400 Protocol and X.500 Standard Conventions.

A2.2.1. Originator/Recipient (O/R) Address. Use the format in **Table A2.2.** to fill in the O/R address string variables.

Table A2.2. Originator/Recipient (O/R) Address String.

ou2=mailbox
prmd=dms+gov+sipr (SIPRNET accounts only)
o = ST1 (i.e., two letter state abbreviation and # is a sequence number)
ou1 = geographic reference code number (georefcode##)
c = us
a = DMS

A2.2.1.1. Set the defaults for the "o" and "ou1" values to o=ST# where ST is the two-letter state abbreviation and # is a sequence number. Set "1" as the first location in the state and subsequent sites will have higher numbers. The ou1=XXXX## where the XXXX is the four-character geo-graphical reference code and the ## is once again a sequence number based on the number of DMS X.400 message transfer agent addresses at a given location.

A2.2.1.2. The c=US and ADMD=DMS values are automatic defaults for DMS servers and are created when the X.400 connector is created during the entry of DMS users.

A2.2.1.3. Ensure the X.500 O/R address is the same as the X.400 O/R address or the DMS User Agent (client) cannot process military elements of service (P42/P772) messaging.

A2.2.2. DELETED.

A2.2.2.1. DELETED.

A2.2.2.2. DELETED.

A2.2.2.3. DELETED.

A2.2.2.4. DELETED.

A2.2.3. Organizational Display Naming Convention. The recommended format for the organizational display name conforms to the SMTP organization common name convention. (e.g., ACC/SE Safety Office).

A2.2.4. Individual Display Naming Convention. This individual display name format is required to preposition the Air Force for future directory synchronization and standardization efforts. The recommended format for the individual display name conforms to the SMTP individual CN convention.

A2.2.5. Alias Naming Convention. Use the same alias as the UserID portion of the SMTP address convention (FirstName**.**LastName). For example, Robert Smith is represented by bob**.**smith. The system administrator should set the alias to default to this convention. Whatever appears in the alias field will automatically create the default SMTP address.

A2.2.6. Recommended OU Naming Methodology. The recommended OU naming methodology is to follow organizational structures: "OrganizationName" for OUs used as organizational TSSs and "OfficeSymbol" for OUs used as offices.

A2.2.6.1. A space should exist after all numbers (e.g., “1 TFW” for the Organizational-level OU and “CC” for the subordinate Office-level OU).

A2.2.6.2. Organizations that are of the format “Det 1 AFRL,” will use “AFRL Det 1.”

A2.2.6.3. Organizations that have no specific unit designation will be preceded with the installation name (e.g., Gunter Red Cross).

A2.2.7. DMS Messaging Objects. These objects represent individuals, organizations, or offices.

A2.2.7.1. Messaging objects for people are created using the ACP120/dmsOrganizationaPerson (**Table A2.3.**) or DODPKIUser/MGS (**Table A2.4.**) objects.

A2.2.7.1.1. DmsOrganizationalPerson Object. This object will be used to create individual entries (e.g., Lt Gen John Doe) in the DMS directory and is normally limited to high-ranking officials on an installation/base.

Table A2.3. DmsOrganizationalPerson Object.

Field	Description
Surname [Mandatory]	Fill in legal last name. Punctuation is not permitted (except apostrophes and a hyphen as commonly used in married name).
Description [Mandatory]	“LastName, FirstName MiddleInitial GenerationQualifier Rank Organization/Office.” “Known-by” name may be substituted for first name but not Nicknames. Punctuation is not permitted (except comma after last name, apostrophes, and a hyphen as commonly used in married name). Rank must conform to the Rank format. It is acceptable for contractors to have the military office symbol of the office they support.
Internet Address [Optional]	The SMTP address will be set with the SMTP standard username format.

X400 Address [Mandatory]	O/R Address. Use the DMS sub-registration authority (SRA) format listed below to fill in the O/R address string variables:
	ou2 = mailbox
	PRMD = DMS+GOV+SIPR (SIPRNET accounts only)
	o= ST1 (i.e., two letter state abbreviation and # is a sequence number)
	ou1 = geographic reference code number (georefcode##)
	c = us
	a = DMS

Street Address [Optional]	Enter the address of the user’s work location. Include Army/Air Force Post Office (APO) for outside the continental US (OCONUS). For organizational users leave blank.
Locality Name [Mandatory]	Enter the duty location (e.g., Maxwell, Langley, Pentagon, etc.) or city if no base exists.
State [Mandatory]	Enter the state portion of the user’s work location in 2-letter state code.

Field	Description
Postal Code [Optional]	Enter the zip code of the user's work location.
Organizational Unit [Mandatory]	Enter the organization of the user in abbreviated format.
Telephone [Optional]	Enter the DSN phone number. Do not include the country code. Do not include "DSN."
Business Telephone 2 [Optional]	Enter the commercial phone number. Include the area or country code. Either the US or European format may be used; e.g., "(999) 999-9999" or "999.999.9999." Foreign phone numbers are allowed.
Rank [Mandatory]	Rank must conform to the rank format.
Delivery Office [Optional]	Enter the office symbol (e.g., "SC").
Title [Optional]	Description of position.
Business Category [Mandatory]	Enter "AD" for Active Duty, "ANG" for Guard, "AFRC" for Reserves, "Ctr" for Contract personnel, "Civ" for Civilians.
Common Name [Mandatory]	**"**LastName, FirstName MiddleInitial GenerationQualifier. "Known-by" name may be substituted for first name but not Nicknames. Tiebreaker will be the middle name spelled. If a tie still exists, then the rank and office symbol will serve to uniquely identify the individual (e.g., O'Grady, Joseph Ernest Jr TSgt ACC/SCB). Rank must conform to the rank format.
V3 Certificate [Mandatory]	Post the individual's HGS V3 digital signature and encryption certificates, if created.
See Also [optional]	Distinguished name (DN) of other DMS entry that may be used if person is unavailable.
Garrison [optional]	DN of Deployed entry if the person is deployed and can be reached by another DMS DN.

A2.2.7.1.2. DODPKIUser (MGS). This object will be used to create individual entries in the DMS Directory and will support MGS messaging.

Table A2.4. DODPKIUser (MGS) Object.

Field	Description
Common Name [Mandatory]	"LastName, FirstName MiddleInitial GenerationQualifier. "Known-by" name may be substituted for first name but not Nicknames. Tiebreaker will be the middle name spelled. If a tie still exists, then the rank and office symbol will serve to uniquely identify the individual. (e.g., O'Grady, Joseph Ernest Jr TSgt ACC/SCB). Rank must conform to the rank format as outlined in paragraph **5.1.5.4.1.**
Surname [Mandatory]	Fill in legal last name. Punctuation is not permitted (except apostrophes and a hyphen as commonly used in married name).
Organizational Unit [Mandatory]	Enter the organization and office in abbreviated format "Organizations/ Office."
Organization Name [Optional]	Enter the MAJCOM the individual is assigned in abbreviated format.
Given Name [Mandatory]	Fill in legal first name. Leave blank for objects that are not people. Nicknames or "Known-by" name may not be used.
Initials [Mandatory]	Fill in legal middle initial. Leave blank for individuals who don't have a middle name.
Description [Mandatory]	"LastName, FirstName MiddleInitial GenerationQualifier Rank Organization/Office". "Known-by" name may be substituted for first name but not Nicknames. Punctuation is not permitted (except comma after last name, apostrophes, and a hyphen as commonly used in married name). Rank must conform to the Rank format. It is acceptable for contractors to have the military office symbol of the office they support.
Preferred form of Full Name [Optional]	The format for full name follows the description name format.
Internet Address [Optional]	The SMTP address will be set in accordance with the standard SMTP username of "org.office@base.af.mil" (e.g., "ACC/SE Safety" would become "acc.se@base.af.mil"). Spaces and punctuation are not permitted. If necessary for uniqueness they can be extended to a third component that includes description (e.g., "ACC/SE Safety" would become "acc.se.safety").
Postal Address [Optional]	Enter the address of the user's work location. Include APO for OCONUS. For organizational users leave blank.
Locality Name [Mandatory]	Enter the duty location (e.g., Maxwell, Langley, Pentagon, etc.) or city if no base exists.
State [Mandatory]	Enter the state portion of the user's work location in 2-letter state code.
Postal Code	Enter the zip code of the user's work location.
Telephone [Optional]	Enter the DSN phone number. Do not include the country code. Do not include "DSN."

Field	Description
Business Telephone 2 [Optional].	Enter the commercial phone number. Include the area or country code. Either the US or European format may be used; e.g., "(999) 999-9999" or "999.999.9999." Foreign phone numbers are allowed.
FAX [optional]	Enter FAX in DSN format. If the FAX only has a commercial number, then the commercial number may be used.
Delivery Office [Optional]	For individual users, enter the Office Symbol (e.g., "SC"). For organizational users, leave blank.
Duty Title [Optional]	Description of position.
Department [Optional].	Enter the user's Office Symbol.
Business Category [Mandatory].	Enter "AD" for Active Duty, "ANG" for Guard, "AFRC" for Reserves, "Ctr" for Contract personnel, "Civ" for Civilians.
User SMIME Certificate [Optional]	If the user possesses an MGS certificate it can be posted into the user Secure Multipurpose Internet Mail Extension (SMIME) certificate attribute for use.

A2.2.7.2. Organizations and offices are created using the dmsOrganizationalUnit (**Table A2.5.**), and dmsOrganizationalRoles (**Table A2.6.**).

A2.2.7.2.1. DmsOrganizationalUnit Object. This object will be used to create entries for Organizations and Offices in the DMS directory.

Table A2.5. DmsOrganizationalUnit Object.

Field	Description
Description [Mandatory]	"Organization/Office ShortDescriptionOfOffice" (e.g., "ACC/SE Safety"). A space must exist after all numbers in display name (e.g., "1 FW/CC Command Section"). Organizations that are of the format "Det 1 AFRL," will use "AFRL Det 1." Leading acronyms (e.g., "HQ") will not be used. Organizations with no specific unit designation will be preceded with the base name (e.g., "Gunter Red Cross").
Internet Address [Optional]	The SMTP address will be set in accordance with the standard SMTP username of "org.office@base.af.mil" (e.g., "ACC/SE Safety" would become "acc.se@base.af.mil"). Spaces and punctuation are not permitted. If necessary for uniqueness they can be extended to a third component that includes description (e.g., "ACC/SE Safety" would become "acc.se.safety").
PLA Name [Optional]	Enter the organizations plain language address (PLA). For offices, enter the PLA and "//[OfficeSymbol//" (e.g., 1 FW MINOT ND//CC//).

X.400 Address [Mandatory]	O/R) Address. Use the DMS SRA format listed below to fill in the O/R address string variables:
	ou2 = mailbox
	prmd = dms+gov+SIPR (SIPRNET accounts only)
	o= ST1 (i.e., two letter state abbreviation and # is a sequence number)
	ou1 = geographic reference code number (georefcode##)
	c = us
	a = DMS

Street Address [Optional]	Enter the street address of the user's work location. Include APO for OCONUS. For organizational users leave blank.
Locality Name [Mandatory]	Enter the duty location (e.g., Maxwell, Langley, Pentagon, etc.) or city if no base exists.
State [Mandatory]	Enter the 2-letter state code.
Postal Code [Optional]	Enter the zip code.
Business Category [Mandatory]	Enter "AD" for Active Duty, "ANG" for Guard, "AFRC" for Reserves, "Contractor" for Contractors, and CIV for Civilians.
Telephone [Optional]	Enter the DSN Phone number for the individual or organizational user (e.g., "999-9999"). Do not include the country code. Do not include "DSN".
Business Telephone [Optional]	Enter the commercial phone number. Include the area or country code. Either the US or European format may be used; e.g., "(999) 999-9999" or "999.999.9999." Foreign phone numbers are allowed.

Field	Description
FAX [Optional]	Enter the DSN FAX number. If the FAX only has a commercial number, then the commercial number may be used.
Delivery Office [Optional]	Enter the Office Symbol (e.g., “SC”).
Organizational Unit [Mandatory]	For top-level organization entries, enter the organization. For office accounts, enter the office symbol.
Garrison [Optional]	DN of entry in deployed DIT that represents the unit in a deployed environment.
Associated PLA [Mandatory]	DN of GENSER PLA that represents the roles organization in AUTODIN.
See Also [Optional]	DN of entry (normally office).
V3 Certificate [Mandatory]	Post the V3 Signature, Encryption and Transitional Certificate.
KmandSigCertificate [Mandatory]	Post the V1 certificate if created.

A2.2.7.2.2. DmsOrganizationalRole Object. This object will be used to create roles (e.g., Superintendent, Officer-in-Charge [OIC], Noncommissioned Officer-in-Charge [NCOIC]) in the DMS Directory and is normally subordinate to an office entry (**Table A2.6.**). Sibling certificates are created for roles.

Table A2.6. DmsOrganizationalRole Object.

Field	Description
Description [Mandatory]	Enter the long format of the duty title or Role being represented (e.g., Superintendent, DMS-AF Registration Branch).
Internet Address [Optional].	The SMTP address will be set in accordance with the standard SMTP username of "org.office@base.af.mil" (e.g., "ACC/SE Safety" would become "acc.se@base.af.mil"). Spaces and punctuation are not permitted. If necessary for uniqueness they can be extended to a third component that includes description (e.g., "ACC/SE Safety" would become "acc.se.safety").

X.400 Address [Mandatory]	O/R Address. Use the DMS SRA format listed below to fill in the O/R address string variables:
	ou2 = mailbox
	prmd = dms+gov+SIPR (SIPRNET accounts only)
	o= ST1 (i.e., two letter state abbreviation and # is a sequence number)
	ou1 = geographic reference code number (georefcode##)
	c = us
	a = DMS

Street Address [Optional]	Enter the street address of the user's work location. Include APO for OCONUS. For organizational users leave blank.
Locality Name [Mandatory]	Enter the duty location (e.g., Maxwell, Langley, Pentagon, etc.) or city if no base exists.
State [Mandatory]	Enter the 2-letter state code.
Postal Code [Optional]	Enter the zip code.
Business Category	Enter the "Type" organization as listed in the "Type Organization descriptors (Keywords)" listing.
Telephone [Optional]	Enter the DSN phone number. Do not include the country code. Do not include "DSN."
Business Telephone 2 [Optional]	Enter the commercial phone number. Include the area or country code. Either the US or European format may be used; e.g., "(999) 999-9999" or "999.999.9999." Foreign phone numbers are allowed.
FAX [Optional]	Enter the DSN FAX number. If the FAX only has a commercial number, then the commercial number may be used.
Delivery Office [Optional]	Enter the Office Symbol (e.g., "SC").
Organizational Unit [Mandatory]	Enter the organization and office of the role "Organization/Office."

Field	Description
Common Name [Mandatory]	**"**Duty Title." (e.g., NCOIC, Superintendent, OIC). Duty Title should be entered in short form. Do not attempt to provide a full descriptive duty title. The full form of the duty title will be addressed in the Description attribute.
V3 Certificate [Mandatory]	Post the individuals HGS V3 digital signature and encryption certificates if created.
Role Occupant [Optional]	DN of individual filling role (if one exists).
PLA Name [Mandatory]	AUTODIN PLA//OfficeSymbol// (e.g., 42 AW MAXWELL AFB AL for organization, or 42 AW MAXWELL AFB AL//CC// for offices.
Associated PLA [Mandatory]	DN of AUTODIN PLA listed in GENSER PLA subtree.
See Also [Optional]	DN of organization or office.
BackPointers [Optional]	DN of Mail Lists, organization, or office.

Attachment 3

MARKING CLASSIFIED ELECTRONIC MESSAGES

A3.1. Marking Classified Electronic Messages. Mark all classified electronic messages with a level of classification equivalent to the information they contain or reveal.

A3.1.1. Mark all electronic messages on classified networks by entering the appropriate classification in parenthesis by using these symbols: "(S)" for SECRET, "(C)" for CONFIDENTIAL, and "(U)" for UNCLASSIFIED, as the first marking in the "Subject" box of the message template. Following the subject, place the appropriate symbol indicating the appropriate classification of the subject itself. Do not send classified messages or mark messages as classified on an unclassified network.

A3.1.2. Users will select the appropriate message classification from the pull-down menu.

A3.1.3. Begin the text of the message on the third line (i.e., leave one blank line between the classification marking and the beginning of the message text).

A3.1.4. Use abbreviated classification symbol at the beginning of all paragraphs and subparagraphs.

A3.1.5. Indicate the security classification of any attachments by placing the abbreviated classification symbol in parentheses before the attachment icon. If the message is unclassified without the attachments, then add this mandatory line: "THIS MESSAGE IS UNCLASSIFIED WHEN SEPARATED FROM ATTACHMENT."

A3.1.6. Place Critical Nuclear Weapon Design Information, Cryptographic, Restricted Data, or other designators indicating special handling in the text following the security classification. Place markings for RESTRICTED DATA-ATOMIC ENERGY ACT 1954, and FORMERLY RESTRICTED DATA ATOMIC ENERGY ACT on the message as shown in DOD 5200.1-PH; AFPD 31-4, *Information Security*; and AFI 31-401.

A3.2. Reply and Forward Actions.

A3.2.1. Reply and forward actions carry the highest classification of any information contained within the appended electronic messaging transmissions.

A3.2.2. Text markings included in a "Reply/Forward" will follow instructions listed above.

A3.2.3. If comments included in a "Reply/Forward" change the classification level of the electronic messaging transmission, then change the classification symbol of the "Subject" box and message text markings accordingly.

Attachment 4

TRANSMITTING UNCLASSIFIED INFORMATION ON CLASSIFIED NETWORKS

A4.1. Transmitting Unclassified Information on Classified Networks. Use the following guidelines for all unclassified messages sent across any network cleared for classified material.

A4.1.1. Mark unclassified electronic messaging messages sent across classified networks by entering the symbol "(U)" in parenthesis as the first marking in the "Subject" box of the message.

A4.1.2. Users will select the appropriate message classification from the pull-down menu.

A4.1.3. Identify any special messaging handling requirements (i.e., "Pass To" and "For").

A4.1.4. Identify the "From" (message originator) and "To" (message recipients) addresses.

A4.1.5. Begin the text of the message after all required administrative information identified above.

A4.1.6. Attachments included in an unclassified message transmission do not need to have the classification noted.

NOTE: If an attachment is classified, the entire electronic messaging transmission is classified.